

In re Patent Application of
MARINET ET AL.
Serial No. 09/995,258
Filed: NOVEMBER 27, 2001

In the Claims:

This listing of claims replaces all prior versions and listing of claims in the application.

Claims 1-16 (canceled).

17. (Previously presented) A random signal generator comprising:

an electronic noise source comprising a folded MOS transistor having a drain-source current with a random component; and

a circuit for generating a digital signal based upon the random component.

18. (Previously presented) A random signal generator according to Claim 17, wherein said folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being S-shaped and having a size that is at a resolution limit based upon manufacturing technology.

19. (Previously presented) A random signal generator according to Claim 17, wherein said folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being zigzag-shaped and having a size that is at a resolution limit based upon manufacturing technology.

20. (Previously presented) A random signal generator according to Claim 17, further comprising a reference transistor connected to said folded MOS transistor, said reference transistor receiving a gate voltage and a bias current equal to a gate voltage and a bias current applied to

said folded MOS transistor for causing the drain-source current therefrom to randomly vary.

21. (Previously presented) A random signal generator according to Claim 17, further comprising a comparison circuit for comparing the randomly varying drain-source current to a detection current.

22. (Previously presented) A random signal generator according to Claim 21, wherein said comparison circuit determines a difference between the randomly varying drain-source current and the detection current; and further comprising an amplifier for amplifying the difference.

23. (Previously presented) A random signal generator according to Claim 17, wherein said circuit comprises a sampling circuit for sampling the digital signal for providing a random digital word.

24. (Previously presented) A random signal generator according to Claim 17, further comprising an integrating circuit for maintaining a gate voltage on said folded MOS transistor within a desired range of values.

25. (Previously presented) A random signal generator circuit comprising:

- a plurality of random signal generators, each random signal generator comprising

- an electronic noise source comprising a folded MOS transistor having a drain-source current with a random component, and

- a circuit for generating a digital signal based upon the random component; and

a logic circuit connected to said plurality of random signal generators for combining the digital signals for generating a digital number.

26. (Previously presented) A random signal generator circuit according to Claim 25, wherein each folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being S-shaped and having a size that is at a resolution limit based upon manufacturing technology.

27. (Previously presented) A random signal generator circuit according to Claim 25, wherein each folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being zigzag-shaped and having a size that is at a resolution limit based upon manufacturing technology.

28. (Previously presented) A random signal generator circuit according to Claim 25, wherein each random signal generator further comprises a reference transistor connected to said folded MOS transistor, said reference transistor receiving a gate voltage and a bias current equal to a gate voltage and a bias current applied to said folded MOS transistor for causing the drain-source current therefrom to randomly vary.

29. (Previously presented) A random signal generator circuit according to Claim 25, wherein each random signal generator further comprises a comparison circuit for comparing the randomly varying drain-source current to a detection current.

30. (Previously presented) A random signal generator circuit according to Claim 29, wherein each comparison circuit determines a difference between the randomly varying drain-source current and the detection current; and wherein each random signal generator further comprises an amplifier for amplifying the difference.

31. (Previously presented) A random signal generator circuit according to Claim 25, wherein each circuit comprises a sampling circuit for sampling the digital signal for providing a random digital word; and wherein said logic circuit generates the digital number based upon the random digital word.

32. (Previously presented) A random signal generator circuit according to Claim 25, wherein each random signal generator further comprises an integrating circuit for maintaining a gate voltage on said folded MOS transistor within a desired range.

33. (Previously presented) An integrated circuit comprising:

- a random signal generator circuit for generating a random digital number comprising

- an electronic noise source comprising a folded MOS transistor having a drain-source current with a random component, and

- a logic circuit for generating the random digital number based upon the random component;

- a communications module connected to said random signal generator circuit for transmitting the random digital number to an external terminal; and

- a processor connected to said random signal generator circuit for receiving the generated random digital

number, and for transforming the generated random digital number based upon an authentication function that uses a secret key;

said processor comparing a result of the authentication function to a result of an authentication function provided by the external terminal in response to the random digital number being sent thereto, and authorizing a transaction with the external terminal if the comparison is a match.

34. (Previously presented) An integrated circuit according to Claim 33, wherein the integrated circuit is a portable electronic device.

35. (Previously presented) An integrated circuit according to Claim 34, wherein the portable electronic device comprises a smart card.

36. (Previously presented) An integrated circuit according to Claim 33, wherein said folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being S-shaped and having a size that is that is at a resolution limit based upon manufacturing technology.

37. (Previously presented) An integrated circuit according to Claim 33, wherein said folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being zigzag-shaped and having a size that is that is at a resolution limit based upon manufacturing technology.

38. (Previously presented) An integrated circuit according to Claim 33, further comprising a reference

transistor connected to said folded MOS transistor, said reference transistor receiving a gate voltage and a bias current equal to a gate voltage and a bias current applied to said folded MOS transistor for causing the drain-source current therefrom to randomly vary.

39. (Previously presented) An integrated circuit according to Claim 33, further comprising a comparison circuit for comparing the randomly varying drain-source current to a detection current.

40. (Previously presented) An integrated circuit according to Claim 39, wherein said comparison circuit determines a difference between the randomly varying drain-source current and the detection current; and further comprising an amplifier for amplifying the difference.

41. (Previously presented) An integrated circuit according to Claim 33, further comprising an integrating circuit for maintaining a gate voltage on said folded MOS transistor within a desired range of values.

42. (Previously presented) A method for generating a random number from an electronic noise source, the method comprising:

providing a folded MOS transistor having a drain-source current with a random component;

generating a random digital signal based upon the random component.

43. (Previously presented) A method according to Claim 42, wherein the folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the

channel being S-shaped and having a size that is at a resolution limit based upon manufacturing technology.

44. (Previously presented) A method according to Claim 42, wherein the folded MOS transistor comprises a drain and a source with a channel defined therebetween, with the channel being zigzag-shaped and having a size that is at a resolution limit based upon manufacturing technology.

45. (Previously presented) A method according to Claim 42, further comprising:
providing a reference transistor connected to the folded MOS transistor; and
providing a gate voltage and a bias current to the reference transistor, the gate voltage and the bias current being equal to a gate voltage and a bias current applied to the folded MOS transistor for causing the drain-source current therefrom to randomly vary.

46. (Previously presented) A method according to Claim 42, further comprising comparing the randomly varying drain-source current to a detection current.

47. (Previously presented) A method according to Claim 46, wherein the comparing comprises determining a difference between the randomly varying drain-source current and the detection current; and further comprising amplifying the difference.

48. (Previously presented) A method according to Claim 42, wherein the sampling comprises providing a random digital signal based upon the sampled random binary signal, and further comprising generating the random number based upon the random digital signal.

In re Patent Application of
MARINET ET AL.
Serial No. 09/995,258
Filed: NOVEMBER 27, 2001

49. (Previously presented) A method according to Claim 42, further comprising maintaining a gate voltage on the folded MOS transistor within a desired range of values.